UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/688,019	10/17/2003	Terence Spies	ID-10	2185

36532 7590 11/29/2005

G. VICTOR TREYZ
FLOOD BUILDING
870 MARKET STREET, SUITE 984
SAN FRANCISCO, CA 94102

EXAMINER	
CHEN, SHIN HON	
ART UNIT	**PAPER NUMBER**
2131	

DATE MAILED: 11/29/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/688,019	SPIES ET AL.	
	Examiner	Art Unit	
	Shin-Hon Chen	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *15 March 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-28* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-28* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *17 October 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *3/15/04*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-28 have been examined.

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1-12, 14-16, 18, and 21-27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gentry et al. U.S. Pub. No. 20030179885 (hereinafter Gentry) in view of Goh et al. U.S. Pat. No. 20050102512 (hereinafter Goh) and further in view of Forman U.S. Pub. No. 20030120733 (hereinafter Forman).

4. As per claim 1, Gentry discloses a method for controlling communications in an identity-based encryption (IBE) system in which a message encrypted using an IBE public key of a recipient is to be sent over a communications network from a sender to the recipient (Gentry: abstract and [0011]), wherein the recipient is in a district associated with an IBE private key generator from which the recipient obtains an IBE private key for decrypting the message encrypted with the IBE public key (Gentry: [0011]), comprising: at the IBE private key generator, providing district policy information to the sender over the communications network (Gentry: [0011] and [0029] and [0032]: the root key generation parameter); and at the sender, using the district policy information in sending the message to the recipient (Gentry: [0013] and [0032]: use the parameter to encode message for recipient). Furthermore, Goh discloses the

sender receives policy from a trusted authority prior to sending a message to a recipient (Goh: [0024]). It would have been obvious to one having ordinary skill in the art to allow the sender to receive parameter or information regarding the recipient in determining the method of encrypting the message because they are both applied in the IBE scheme. Therefore, it would have been obvious to one having ordinary skill in the art at the time of applicant's invention to combine the teachings of Goh within the system of Gentry because it allows the sender to derive the encryption method and key for the message encryption. Gentry as modified does not explicitly disclose using the district policy to determine whether to send the message to the recipient. However, Forman discloses the sender is able to receive from a server the status of a recipient and determine whether to send the message to the recipient (Forman: [0014]-[0015]). It would have been obvious to one having ordinary skill in the art to allow the sender to receive necessary information regarding transmission of message according to policies. Therefore, it would have been obvious to one having ordinary skill in the art at the time of applicant's invention to combine the teachings of Forman within the combination of Gentry-Goh because it prevents sender from wasting time and effort in composing a message that is not according will not reach the recipient.

5. As per claim 2, Gentry as modified discloses the method defined in claim 1. Gentry as modified further discloses wherein using the district policy information at the sender comprises using the district policy information to determine whether to send the message to the recipient. Goh discloses the sender receives policy from a trusted authority prior to sending a message to a recipient (Goh: [0024]).

6. As per claim 3, Gentry as modified discloses the method defined in claim 1. Gentry as modified further discloses wherein using the district policy information at the sender comprises using the district policy information and client policy information to determine whether to send the message to the recipient (Goh: [0047]-[0048]: district policy; Forman: [14]-[0015]: client policy).

7. As per claim 4, Gentry as modified discloses the method defined in claim 1. Gentry as modified further discloses wherein using the district policy information at the sender comprises using the district policy information to determine how to send the message to the recipient (Gentry: [0032]: using the parameter in determining how to encrypt a message).

8. As per claim 5, Gentry as modified discloses the method defined in claim 1. Gentry as modified further discloses wherein the district policy information includes IBE encryption protocol information, the method comprising using the IBE encryption protocol information at the sender to determine which IBE encryption protocols are being used by the district (Gentry: [0029] and [0032]; Goh: [0048]-[0049]).

9. As per claim 6, Gentry as modified discloses the method defined in claim 1. Gentry as modified further discloses wherein the district policy information includes IBE public key format information, the method comprising using the IBE public key format information from the

district policy information at the sender to determine how to construct the IBE public key (Goh: [0047]-[0048]).

10. As per claim 7, Gentry as modified discloses the method defined in claim 1. Gentry as modified further discloses wherein the recipient has a username and wherein the district policy information includes IBE public key format information that specifies which portion of the recipient's username is used to form the IBE public key, the method comprising using the IBE public key format information from the district policy information at the sender to construct the IBE public key from the recipient's username (Gentry: [0011] and [0032]: the parameter information and the recipient's identity information to encrypt message).

11. As per claim 8, Gentry as modified discloses the method defined in claim 1. Gentry as modified further discloses wherein the district policy information includes communications protocol information that specifies which communications protocols are used by the district, the method comprising using the communications protocol information at the sender to determine which communications protocols are being used by the district (Gentry: [0013]: determine if other lower-level key generation parameters are involved).

12. As per claim 9, Gentry as modified discloses the method defined in claim 1. Gentry as modified further discloses wherein the district policy information includes communications protocol information that specifies which communications protocols are used by the district, the

method comprising using the communications protocol information at the sender to determine which message format is being used by the district (Gentry: [0029] and [0032]).

13. As per claim 10, Gentry as modified discloses the method defined in claim 1. Gentry as modified further discloses wherein the district policy information includes authentication protocol information that specifies what type of authentication is required before the IBE private key generator for the district provides IBE private keys to recipients in the district, the method comprising using the authentication protocol information at the sender in sending the message to the recipient (Goh: [0055]).

14. As per claim 11, Gentry as modified discloses the method defined in claim 1. Gentry as modified further discloses wherein the district policy information includes authentication protocol information that specifies what type of authentication is required before the IBE private key generator for the district provides IBE private keys to recipients in the district, the method comprising using the authentication protocol information at the sender to determine whether to send the message to the recipient (Forman: [0014]-[0015]).

15. As per claim 12, Gentry as modified discloses the method defined in claim 1. Gentry as modified further discloses wherein the district policy information includes authentication protocol information that specifies what type of authentication is required before the IBE private key generator for the district provides IBE private keys to recipients in the district, the method comprising using the authentication protocol information at the sender to determine whether the

recipient uses a smart card when being authenticated by the IBE private key generator (Goh: [0092]: when smartcard is involved).

16. As per claim 14, Gentry as modified discloses the method defined in claim 1. Gentry as modified further discloses wherein the district comprises multiple subdistricts, each of the multiple subdistricts having its own respective subdistrict IBE private key generator, wherein the recipient is associated with at least one of the subdistricts, and wherein each subdistrict has associated subdistrict policy information, the method further comprising: at the sender, obtaining the subdistrict policy information for each of the multiple subdistricts; and at the sender, using the subdistrict policy information for the multiple subdistricts in sending the message to the recipient (Gentry: [0013]: hierarchical identity-based system).

17. As per claim 15, Gentry as modified discloses the method defined in claim 1. Gentry as modified further discloses wherein the district comprises multiple subdistricts, each of the multiple subdistricts having its own respective subdistrict IBE private key generator, wherein the recipient is associated with more than one of the subdistricts, and wherein each subdistrict has associated subdistrict policy information, the method further comprising: at the sender, obtaining the subdistrict policy information for each of the multiple subdistricts; and at the sender, using the subdistrict policy information for the subdistricts with which the recipient is associated in determining which subdistrict to send the message to (Gentry: [0013]).

18. As per claim 16, Gentry as modified discloses the method defined in claim 1. Gentry as modified further discloses wherein the district comprises multiple subdistricts, each of the multiple subdistricts having its own respective subdistrict IBE private key generator, wherein the recipient is associated with more than one of the subdistricts, wherein the subdistricts use different techniques for authenticating recipients, wherein each subdistrict has associated subdistrict policy information that specifies the techniques used for authenticating their recipients, the method further comprising: at the sender, obtaining the subdistrict policy information for each of the multiple subdistricts; and at the sender, using the subdistrict policy information for those subdistricts with which the recipient is associated in determining which of those subdistricts to send the message to based on which technique is used to authenticate the recipient at each of those subdistricts (Gentry: [0013]-[0014]).

19. As per claim 18, Gentry as modified discloses the method defined in claim 1. Gentry as modified further discloses wherein using the district policy information comprises: at the sender, using the district policy information to determine whether to display a notice for the sender (Forman: [0015]).

20. As per claim 21-27, claims 21-27 encompass the same scope as claims 1-20. Therefore, claims 21-27 are rejected based on the reasons set forth in rejecting claims 1-20.

21. Claims 13 and 17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gentry in view of Goh and further in view of Forman and further in view of Klos et al. U.S. Pub. No. 20050015449 (hereinafter Klos).

22. As per claim 13, Gentry as modified discloses the method defined in claim 1. Gentry as modified does not explicitly disclose wherein the district policy information includes content-based protocol information that specifies how messages are to be handled based on their content, the method comprising using the content-based protocol information at the sender to determine whether to send the message to the recipient. However, Klos discloses content-based filtering is well known in e-mail communication system (Klos: [0016]). It would have been obvious to one having ordinary skill in the art to inform the sender of recipient policy and status. Therefore, it would have been obvious to one having ordinary skill in the art at the time of applicant's invention to combine the teachings of Klos within the combination of Gentry-Goh-Forman because it allows the user to determine whether he/she should send undeliverable message to a recipient based on the policy information.

23. As per claim 17, Gentry as modified discloses the method defined in claim 1. Gentry as modified does not explicitly disclose wherein the message has certain message content and wherein using the district policy information comprises, at the sender, determining whether to send the message to the recipient based on the message content and the district policy information. However, Klos discloses content-based filtering is well known in e-mail communication system (Klos: [0016]). It would have been obvious to one having ordinary skill

in the art to inform the sender of recipient policy and status. Therefore, it would have been obvious to one having ordinary skill in the art at the time of applicant's invention to combine the teachings of Klos within the combination of Gentry-Goh-Forman because it allows the user to determine whether he/she should send undeliverable message to a recipient based on the policy information.

24. Claims 19 and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gentry in view of Goh and further in view of Forman and further in view of Arcuri et al. U.S. Pub. No. 20040162879 (hereinafter Arcuri).

25. As per claim 19, Gentry as modified discloses the method defined in claim 1. Gentry as modified does not explicitly disclose wherein providing the district policy information to the sender comprises providing the district policy information in the form of a district policy information list containing an identifier for each list entry. However, Arcuri discloses that e-mail rules can be in the form of policy information list (Arcuri: [0057]). It would have been obvious to one having ordinary skill in the art to allow users to provide the policy information list so that the server can keep track of the status of the recipient and notify sender of the status. Therefore, it would have been obvious to one having ordinary skill in the art at the time of applicant's invention to combine the teachings of Arcuri within the combination of Gentry-Goh-Forman because it allows the sender to determine whether to send the message.

26. As per claim 20, Gentry as modified discloses the method defined in claim 1. Gentry as modified does not explicitly disclose wherein providing the district policy information to the sender comprises providing the district policy information in the form of a district policy information list having list entries, wherein at least some of the list entries are digitally signed. However, Arcuri discloses that e-mail rules can be in the form of policy information list (Arcuri: [0057]). It would have been obvious to one having ordinary skill in the art to allow users to provide the policy information list so that the server can keep track of the status of the recipient and notify sender of the status. Therefore, it would have been obvious to one having ordinary skill in the art at the time of applicant's invention to combine the teachings of Arcuri within the combination of Gentry-Goh-Forman because it allows the sender to determine whether to send the message. Although Arcuri does not explicitly disclose some of the list entries are digitally signed. However, it would have been obvious to one with ordinary skill in the art to digitally sign the rules so that the sender can trust the authenticity of the e-mail rules.

Conclusion

27. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Schoen et al. U.S. Pub. No. 20030204722 discloses instant messaging apparatus and method with instant messaging secure policy certificates.

Cook et al. U.S. Pub. No. 20040139314 discloses considering preferences of sender and recipient prior to communicating messages.

Bouchard U.S. Pub. No. 20030115448 discloses method for securely communicating a message.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Shin-Hon Chen whose telephone number is (571) 272-3789. The examiner can normally be reached on Monday through Friday 8:30am to 5:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Shin-Hon Chen
Examiner
Art Unit 2131

SC

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100